



República Federativa do Brasil
Ministério da Economia
Instituto Nacional da Propriedade Industrial

(11) PI 1014882-5 B1



(22) Data do Depósito: 23/04/2010

(45) Data de Concessão: 29/09/2020

(54) Título: MÉTODO E SISTEMA DE TRANSAÇÃO DE PAGAMENTO ELETRÔNICO, EM PARTICULAR MEDIANTE O USO DE MEIO DE PAGAMENTO SEM CONTATO

(51) Int.Cl.: G06Q 30/00.

(30) Prioridade Unionista: 24/04/2009 SK PP 50024-2009.

(73) Titular(es): LOGOMOTION, S.R.O..

(72) Inventor(es): MIROSLAV FLOREK; MICHAL MASARYK.

(86) Pedido PCT: PCT IB2010051779 de 23/04/2010

(87) Publicação PCT: WO 2010/122520 de 28/10/2010

(85) Data do Início da Fase Nacional: 24/10/2011

(57) Resumo: MÉTODO E SISTEMA DE TRANSAÇÃO DE PAGAMENTO ELETRÔNICO, EM PARTICULAR MEDIANTE O USO DE MEIO DE PAGAMENTO SEM CONTATO. A presente invenção refere-se a um método de transação de pagamento eletrônico caracterizado pelo fato de que, durante o processamento de uma transação de pagamento, uma ligação de comunicação (3) entre o cartão (1) e o terminal (2) é interrompida e o arquivo de resposta ARPC é recebido pelo cartão (1) depois que a ligação de comunicação original (5) é interrompida. Duas fases não separadas por um reinício do cartão (1) em que na segunda fase, dados de pagamento iniciais (ARQC) são utilizados. O arquivo de pagamento ARQC assinado eletronicamente é armazenado na memória do cartão (1) pelo menos até o arquivo de resposta ARPC de tempo correspondente ser recebido e processado. A solução permite que se posicione o telefone móvel com um cartão de pagamento (1) próximo ao leitor de terminal (2) duas vezes. Na primeira vez, uma solicitação para autorização on-line é gerada, e, durante a o segundo contato, as informações do processador de pagamento (5) são registradas no pedido de pagamento.

Relatório Descritivo da Patente de Invenção para **"MÉTODO E SISTEMA DE TRANSAÇÃO DE PAGAMENTO ELETRÔNICO, EM PARTICULAR MEDIANTE O USO DE MEIO DE PAGAMENTO SEM CONTATO"**.

Campo da Invenção

5 A presente invenção refere-se a um procedimento e um sistema de um pedido de pagamento eletrônico com o uso de meio de pagamento em uma forma de um cartão de pagamento. Trata-se de um método de um pagamento de uma transação de pagamento de débito direto através da utilização de meio de pagamento sem contato que é ajustado de forma que
10 possa ser inserido em um dispositivo de comunicação móvel.

Situação de tecnologia atual

Terminais POS (ponto de venda) são comumente utilizados para processar transações de pagamento eletrônico utilizando diferentes cartões de pagamento de chip. Estes terminais são conectados a um processador de
15 pagamento remoto sob a forma de um centro de limpeza que pertence a um emissor de cartão de pagamento ou a um banco. No início de um processo de pagamento, o chip do cartão de pagamento é zerado a sua posição inicial. Depois de zerado, a informação sobre o cartão e tipo de terminal será trocada entre o cartão e o terminal. Esta identificação básica traz a conexão
20 entre o cartão e o terminal em uma posição que permite comunicação mútua, bem como comunicação para o servidor de processador de pagamento.

O terminal POS envia dados sobre o pagamento solicitado no cartão, a estrutura de dados inclui, por exemplo, quantidade, moeda corrente, data e semelhantes. O terminal também solicita o cartão de dar uma afirmação. O cartão, de acordo com seus ajustes, gera uma resposta e sinaliza
25 com sua assinatura eletrônica. A resposta do cartão sob a forma de "TC" (Certificado de Transação) significa uma aceitação de pagamento off-line onde a autorização por um processador de pagamento não é necessária. A resposta sob a forma de "ACA" (Criptograma de Autenticação de Aplicação)
30 significa que o pagamento não será aceito pelo cartão sob quaisquer condições. O assunto desta invenção é um método, um procedimento de um processo de pagamento durante geração da resposta sob a forma de ARQC

(Criptograma de Pedido de Autorização). Tal resposta significa que o cartão solicita autenticação e cooperação com o servidor de processador de pagamento.

5 Após uma resposta ser gerada sob a forma de um arquivo de pagamento, principalmente de tipo ARQC, o cartão envia seu arquivo de pagamento criptografado ao processador e espera até a resposta do processador ser recebida. Enquanto espera, o cartão de pagamento precisa ficar em contato com o terminal para criar uma comunicação contínua entre o cartão e o processador de pagamento. A interrupção deste canal causará término
10 do processo de pagamento. Se o processador de pagamento envia de volta um arquivo de resposta ARPC (Criptograma de Resposta de Autorização) no cartão, então o arquivo é enviado através do terminal no cartão de pagamento e o cartão de pagamento decodifica as instruções para procedimento adicional (em particular como ARPC) do arquivo de resposta e reporta o resultado
15 ao terminal sob a forma de TC e eventualmente ACA.

A característica essencial do método de comunicação entre o cartão de pagamento e o processador de terminal/pagamento que é conhecido até agora é uma conexão constante, um contínuo, canal ininterrupto dos dados elementos de hardware de pagamento sem dinheiro durante comunicação bidirecional. A comunicação dura aproximadamente alguns segundos,
20 eventualmente, décimos de segundos. A interrupção da conexão entre o cartão e o terminal causa um novo reinício da aplicação de cartão, que é registrada, por exemplo, através da incrementação de seu contador. A alteração de dados de contato provoca uma mudança de arquivo de pagamento
25 ARQC recém-gerado e após uma interrupção, é possível finalizar o processo de pagamento com sucesso utilizando os dados que foram originalmente gerados antes da conexão ser interrompida. Quando utiliza cartões de pagamento padrão conectado através de um contato, não há problema em manter uma ligação de comunicação confiável visto que esta ligação é inter-
30 rompida apenas no caso em que o cartão é retirado antecipadamente da fenda do leitor apropriado.

Com o aumento de utilização de meio de pagamento sem conta-

to aparece o problema com a estabilidade do canal de comunicação. Não é adequado pedir ao pagador para segurar seu meio de pagamento sem contato de forma ininterrupta com concentração no alcance de um leitor sem contato durante todo o tempo de processo de pagamento. O leitor sem contato geralmente tem uma área limitada de alcance com o propósito de prevenir qualquer interferência com outros dispositivos para diminuir demandas energéticas de criação de campo sem contato e reduzir riscos de segurança. Uma solução que pode ativar um processo de comunicação de pagamento em algumas fases ininterruptas é exigida. Porém, até agora nenhum processo e método que reúne esta demanda é conhecido.

É utilizada uma solução em que um cartão de pagamento sem contato é adaptado também para uma conexão de contato com o terminal. Em tal configuração, a maioria dos pagamentos é realizada através de ligação sem contato entre um cartão de pagamento e um terminal durante o qual o cartão de pagamento não espera por uma resposta do processador de pagamento. Para alcançar comunicação bidirecional entre o cartão e o servidor de processador de pagamento, é necessário que o cartão esteja em conexão de contato com o terminal regularmente, por exemplo, a cada dez pagamentos. Assim, o cartão recebe instruções do processador de pagamento e as executa. Esta configuração diminui o conforto do usuário e acima de tudo exige relação de contato do cartão de pagamento de forma que não seja aplicável para pagamentos que utilizam cartões de pagamento em um dispositivo de comunicação móvel. Não é possível exigir diferentes dispositivos de comunicação móvel, por exemplo, telefones móveis que se conectam com o terminal POS em uma forma de contato.

Antecedentes da invenção

As desvantagens mencionadas acima são eliminadas significativamente por um método de uma transação de pagamento sem contato, em particular com o uso de meio de pagamento sem contato que inclui um método pelo qual após zerar o cartão, o cartão recebe dados de pagamento do terminal de pagamento. Com base nestes dados, um arquivo de pagamento é criado e eletronicamente assinado, principalmente sob a forma de ARQC.

Este arquivo de pagamento é enviado através de um link entre o cartão e o terminal de pagamento ao processador de pagamento, subseqüentemente, o cartão recebe de volta um arquivo de resposta de um processador, principalmente sob a forma de ARPC, que inclui até mesmo dados sobre o arquivo de pagamento original em uma forma decodificada. O cartão processará e decodificará o arquivo de resposta e conseqüentemente decide, define e envia de volta uma declaração afirmativa ou negativa para o pagamento, principalmente na forma TC ou ACA, de acordo com esta invenção, ao terminal. O assunto desta invenção está no fato que durante o cortejo de uma transação de pagamento, a ligação de comunicação entre o cartão e o terminal é interrompida. Esta interrupção pode aumentar basicamente de forma imediata após o arquivo de pagamento ser enviado do cartão ao terminal. A recepção inicial de dados do terminal, geração de um arquivo de pagamento sob a forma de ARQC e seu envio ao terminal dura aproximadamente alguns milésimos de segundo e é realizável durante um posicionamento confortável do cartão perto do leitor de terminal. O arquivo de resposta do processador de pagamento é recebido pelo cartão após a ligação de comunicação original e o terminal se interrompida. As duas fases do processamento de transação de pagamento e a comunicação mencionada são divididas pelo reinício do cartão, enquanto na segunda fase, os dados criados no cartão antes da interrupção da ligação de comunicação entre o cartão e o terminal são utilizados. Um novo reinício do cartão durante uma transação de pagamento é induzida pelo restabelecimento da ligação de comunicação.

O mecanismo de comunicação supracitado pode ser realizado em uma forma segura e ao mesmo tempo com pequenas intervenções em processos comuns de EMV (Europay, MasterCard, VISA) de forma que um arquivo de pagamento assinado eletronicamente, em particular sob a forma de ARQC, seja armazenado na memória do cartão enquanto o arquivo de pagamento é armazenado em uma memória pelo menos até o tempo de recebimento e procedimento de um arquivo de resposta particular de um processador de pagamento, principalmente como ARPC. Armazenamento de um arquivo de pagamento, em particular como ARQC, é uma característica

essencial da solução apresentada, visto que permite dividir o processo de transação de pagamento em fases de forma que a condução de interrupção e procedimento à segunda fase não provoque o cancelamento e fechamento da transação de pagamento em processo.

5 O cartão decodifica o arquivo de resposta recebido, adquire informações sobre um arquivo de pagamento que foi utilizado pelo processador de pagamento durante a criação do arquivo de resposta. Arquivo de pagamento ARQC é decodificado em um arquivo de resposta onde outras instruções e certificados para o cartão podem ser armazenados. O cartão compara o arquivo de pagamento originalmente criado e armazenado em um
10 arquivo de pagamento incluído no arquivo de resposta, subsequente, o cartão cria declarações recusadas e aceitas ao pagamento. A declaração de aceitação para o pagamento é ao cartão condicionada através da igualdade do arquivo de pagamento originalmente criado e armazenado no cartão
15 gerado a partir do arquivo de resposta decodificado. Isto significa que um cartão, na segunda fase de processamento, além de outras informações, também compara o arquivo ARQC armazenado com o arquivo ARQC, que serviu como uma base de ARQC, criado em um processador de pagamento.

 Após receber um arquivo de resposta, o terminal solicita uma re-
20 conexão de uma ligação de comunicação do cartão e do terminal. Após restabelecimento de uma ligação de comunicação do cartão e do terminal, o cartão solicita do terminal, novamente, o envio de dados de pagamento em uma forma de CDOL (Lista de Objeto de Dados de Gerenciamento de Risco de Cartão) que são, em comparação ao CDOL original, adicionados com
25 uma resposta de um processador de pagamento.

 É vantajoso se um cartão de pagamento for incluído em um dispositivo de comunicação móvel, como um telefone móvel. A partir do ponto de vista de expansão possível de tal meio de pagamento, é adequado se o cartão de pagamento estiver localizado em um cartão de memória de tipo
30 micro SD ou mini SD ou SD, visto que telefones móveis comumente têm fendas para introduzir cartões de memória amplos.

 Em um sistema de comunicação de uma fase existente, durante

transação de pagamento, a comunicação regressiva do processador de pagamento para o cartão sempre foi realizada através do mesmo canal de comunicação como foi utilizado no envio do arquivo de pagamento ao processador de pagamento. O novo método apresentado com duas fases capacita a divisão destas fases não apenas a partir do tempo, mas a partir do ponto de vista de hardware. Um caminho de comunicação diferente pode ser utilizado para transferência do arquivo de resposta que foi utilizado para transferir o arquivo de pagamento. Pode ser uma conexão através de uma rede de comunicação móvel à qual dispositivo de comunicação móvel, que abrange o cartão, é registrado. A rede de comunicação móvel é utilizada para enviar o arquivo de resposta entra no cartão através do telefone móvel, que o recebe no formato SMS. Isto pode acontecer depois que o terminal recebeu o arquivo de resposta, mas quando a ligação de comunicação entre o terminal e o cartão não foi restabelecida no limite de tempo presente. Então, o terminal envia informações neste estado ao processador de pagamento e o mesmo organiza o envio do arquivo de resposta ao cartão em uma forma diferente.

É adequado que, no caso do mesmo trajeto de comunicação através do terminal POS ser utilizado, este terminal registre o cartão após receber o arquivo de resposta do processador de pagamento como um terminal com uma identificação que é diferente da identificação do terminal de pagamento na fase em que o arquivo de pagamento foi enviado ao processador de pagamento. Basicamente, isto significa que o terminal com prefixo de identificação diferente dá ao cartão um sinal que tenta conectar como terminal pós-processo com o propósito de finalizar a transação de pagamento já iniciada. Neste tipo de configuração, o terminal mantém o arquivo de resposta como uma preparação para restabelecimento da ligação de comunicação com o cartão.

As desvantagens mencionadas no estado de tecnologia atual são eliminadas também por um método de transação de pagamento sem contato, especialmente com o uso de dispositivo de pagamento sem contato que abrange um cartão de pagamento, um terminal, uma conexão entre o

terminal e o processador de pagamento de acordo com esta invenção. O assunto desta invenção é também no fato que o cartão pagamento é equipado com uma memória para armazenamento do arquivo de pagamento, favoravelmente, um arquivo de pagamento em uma forma de ARQC, em que
5 o arquivo de pagamento é armazenado na memória mesmo depois do cartão ser zerado quando a ligação de comunicação entre o cartão e o terminal é finalizada. O terminal é equipado com uma memória para armazenamento temporário de arquivo de resposta, principalmente sob a forma de ARPC e é ajustado na alteração de seus dados de identificação depois do arquivo de
10 resposta ser recebido. A partir do ponto de vista de alcance exigido é necessário que o cartão de memória para armazenamento de arquivo de pagamento esteja sob a forma de um elemento seguro.

Na configuração vantajosa, o sistema pode ser ajustado de tal forma que o cartão de pagamento esteja no dispositivo de comunicação móvel, de preferência, em um cartão de memória sob a forma de micro SD ou mini SD ou SD e em que o cartão de memória abrange um elemento de comunicação para a conexão com o terminal. Por fazer isto, uma atualização do telefone móvel é alcançada e não apenas para a função do transportador de cartão de pagamento, ou transportador de vários cartões de pagamento,
20 respectivamente, mas também para a criação do canal de comunicação entre o telefone móvel e o terminal. Esta comunicação irá funcionar principalmente em acordo com o padrão NFC.

Descrição dos Desenhos

A invenção é descrita em mais detalhes nas figuras 1 a 5 onde a
25 figura 1 mostra um algoritmo de método existente e conexão para transações de pagamento eletrônico. A figura 2 mostra um algoritmo com duas fases separáveis de processar um pedido de pagamento eletrônico.

A figura 3 representa um esquema de conexão de sistema para uma transação de débito direto sem contato, sobre um telefone móvel equipado com um cartão de pagamento em um cartão de memória inserido que
30 tem uma antena na primeira fase, bem como no pré-processamento. O curso de ordens e um fluxo de arquivos são mostrados a partir do topo da ordem

decrecente.

Na figura 4 existe um esquema de conexão em relação a um esquema de acordo com a figura 3 onde é mostrada a segunda fase pós-processamento com a transferência no cartão através de um terminal. O curso de ordens e um fluxo de arquivos são mostrados a partir do topo da ordem decrecente.

Na figura 5 existe um esquema de conexão relacionado ao esquema mostrado na figura 3, embora aqui seja mostrada a segunda fase, a pós-processamento na versão de transferência ARPC sobre mensagem SMS. O curso de ordens de um fluxo de arquivos é mostrado a partir do topo da ordem decrecente.

Exemplos de aplicação

Exemplo 1

Neste exemplo, o sistema contém um dispositivo de comunicação móvel 4, um terminal 2 com leitor NFC, um servidor de processador de pagamento 5, uma conexão entre o terminal 2 e o servidor de processador de pagamento 5. O dispositivo de comunicação móvel 4 é representado, por exemplo, por telefone móvel NOKIA 6131. O cartão removível 1 com uma memória de formato micro SD é inserida da fenda do dispositivo de comunicação móvel 4. Um cartão de pagamento 1 e também um elemento de comunicação NFC 7 é localizado em um cartão removível 1 com uma memória que tem dimensões padronizadas comuns. O cartão 1 é equipado com uma memória para armazenamento do arquivo de pagamento, com a memória em forma de um elemento seguro, respectivamente em um formato de domínio atual do elemento seguro. O arquivo de pagamento ARQC é armazenado mesmo depois que o cartão 1 é zerado. O reinício do cartão 1 é obtido pela reconexão do cartão 1 ao terminal 2 depois da interrupção de uma ligação e comunicação 3 entre o cartão 1 e o terminal 2 na primeira fase da transação. O terminal 2 é equipado com uma memória para armazenamento temporário do arquivo de resposta, em particular, sob a forma de ARPC. O terminal 2 tem um prefixo de identificação variável; o terminal 2 é ajustado para alterar seus dados de identificação depois que um arquivo de resposta

é recebido. Na primeira fase, o terminal 2 registra como um terminal do tipo 12 (terminal POS 2 ocupado por um vendedor) e na segunda fase como um terminal 2 do tipo 12tc2 ou possivelmente do tipo 27 (terminal pós processamento). A alteração dos servidores de tipo de terminal para correto equilíbrio de mensagens comunicadas, a princípio, pode ser um novo número de tipo do terminal, por exemplo, 27. Em outro caso, quando for problemático introduzir um novo número de tipo do terminal nos sistemas de processamento existente, o mesmo número de tipo 12 e diferente capacidade de terminal podem ser utilizados, aqui é expresso como 12tc2 = 12 com tc diferente – capacidade de terminal. O terminal 2 tem um memória para armazenar um arquivo de resposta ARPC como uma preparação para realização da reconexão da ligação de comunicação 3 com um cartão 1.

Dados sobre um pagamento solicitado quem inclui uma quantidade, moeda corrente e data, são preparados no terminal 2. Estes são incluídos nos dados de CDOL1 (Lista de Objeto de Dados de Gerenciamento de Risco de Cartão). O usuário adota seu telefone móvel ao leitor do terminal 2. Depois que a ligação de comunicação 3 é criada, o terminal 2 solicita ao cartão 1 uma declaração. Na base dos dados recebido, o cartão 1 será criado um arquivo de pagamento na forma do criptograma ARQC. Este arquivo é decodificado por assinatura eletrônica do cartão 1. Durante a ligação de comunicação 3 originalmente criada, um arquivo de pagamento ARQC é transferido em um terminal 2. Depois de sua criação, o arquivo de pagamento ARQC é armazenado no elemento seguro no cartão 1. Depois da transferência do arquivo de pagamento no terminal 2, basicamente não importa se o telefone móvel é ou não movido para longe do leito de terminal 2. É suposto que o telefone seja movido para longe visto que o telefone móvel será segurado pela mão do usuário durante toda a transação de pagamento. O telefone móvel será colocado próximo ao leito de terminal 2 na requisição de terminal 2, ou na realidade, no requerimento de um atendente que monitora todo o curso da transação de pagamento. Depois do primeiro posicionamento, o usuário espera por outra requisição para posicionamento. A ligação de comunicação 3 entre o cartão 1 e o terminal 2 é desconectada quando uma

transação de pagamento está em progresso.

Nesse ínterim, o arquivo de pagamento ARQC é enviado do terminal 2 ao processador de pagamento 5. O processador de pagamento o processa, avalia e junto com outras possíveis instruções, decodifica o arquivo de pagamento ARQC em um arquivo de pagamento na forma do criptograma ARPC. Este arquivo abrange dados decodificados sobre o arquivo de pagamento ARQC. O arquivo de resposta ARPC é recebido pelo cartão 1 de um processador de pagamento 5 depois que a ligação de comunicação original 3 entre o cartão 1 e o terminal 2 é interrompida. Esta interrupção contém um elemento tempo para o momento que separa a primeira e segunda fase do processamento de transação de pagamento. A partir do ponto de visto do cartão 1, estas duas são fases separadas pelo cartão 1 sendo zerado, enquanto os dados criados no cartão durante a primeira fase são utilizados na segunda fase.

O arquivo de pagamento ARQC é armazenado na memória do cartão 1 pelo menos até o momento que o particular arquivo de resposta ARPC do processador de pagamento 5 é recebido e processado. O cartão 1 decodifica o arquivo de resposta ARPC recebido, adquire informações sobre arquivo de pagamento ARQC que foi utilizado por um processador de pagamento 5 quando cria arquivo de resposta ARPC. Depois, o cartão q compara o arquivo de pagamento ARQC armazenado e criado originalmente com o arquivo de pagamento ARQC que é incluído no arquivo de resposta ARPC. Depois desta comparação, o cartão 1 pode fazer uma decisão sobre a sua declaração relativa ao pagamento em processo. Subseqüentemente, o cartão 1 cria uma declaração de aceitação ou rejeição do pagamento sob a forma de TC ou ACA. Declaração de aceitação é criada no cartão 1 sob necessária condição quando o arquivo de pagamento ARQC originalmente criado e armazenado no cartão 1 é idêntico ao arquivo de pagamento ARQC incluído no arquivo de resposta ARPC.

A conexão, conforme descrita neste exemplo, também oferece mais possibilidades da forma como o arquivo de resposta ARPC é transferido ao cartão 1. Se o terminal 2 reporta ao processador de pagamento 5 que

o usuário não posicionou seu telefone móvel próximo ao leitor de terminal 2 pela segunda vez, o processador de pagamento 5 tentará enviar ARPC como dados SMS ao número de telefone determinado ao este cartão de pagamento particular 1. No telefone móvel, o SMS recebido é analisado como dado relevante ao cartão micro SD e inicia a execução de seu próprio terminal POS 2 virtual. A mensagem SMS contém informação sobre o terminal 2 que pertence ao processador de pagamento 4 com prefixo 17 (terminal pós processamento 2, que pertence ao processador de pagamento 5).

Exemplo 2

O processo de uma transação de pagamento on-line é realizado em duas etapas – pré-processamento e pós-processamento. Uma execução de aplicação sem contato, por exemplo, especificação PAYPASS e PAYWAVE pode ser utilizada como um pedido de pagamento. Existem duas aplicações separadas no cartão 1 – PAYPASS/PAYWAVE_POSTPROCESS e PAYPASS/PAYWAVE. As aplicações são localizadas em um domínio seguro e são compatíveis com EMV enquanto compartilham pelo menos três variáveis comuns (Elemento de dados): Contador off-line, Contador de Transação de Aplicação (ATC) e Contador de Última Transação de Aplicação on-line (LATC). A aplicação PAYPASS/PAYWARE armazena temporariamente o valor ARQC, que ela proporciona depois no pós-processamento para a aplicação PAYPASS/PAYWAVE_POSTPROCESS, assim, não tem que contar mais uma vez, pelo tempo salvo. De acordo com esta invenção, um novo tipo de terminal 2 é introduzido: Tipo de terminal = 27 (terminal pós processamento 2).

A solução apresentada capacita posicionar o telefone móvel perto do terminal 2 duas vezes. Na primeira vez, a requisição para uma autorização on-line é gerada e depois do segundo contato, as informações do processador de pagamento 5 é inserida no pedido de pagamento. Se o usuário não posicionar seu telefone móvel pela segunda vez, mas dados relevantes ou um certificado estão na resposta, o terminal 2 reporta ao processador de pagamento 5 que a resposta não foi entregue e o processador de pagamento 5 tentará entregar mais uma vez ao telefone móvel através de SMS – no

caso, do serviço de RESPOSTA SMS é ativado. O caso do usuário ter este serviço, ele pode posicionar seu telefone móvel próximo ao leitor de terminal 2 apenas uma vez também voluntariamente e regularmente. O serviço é ativado durante a primeira instalação de GUI quando GUI reporta ao processador de pagamento 5 através de SMS que RELATÓRIO SMS foi ativado.

O serviço é desabilitado automaticamente quando o processador de pagamento 5, depois de enviar a RESPOSTA SMS, não recebe uma confirmação de sua recepção nos três pagamentos on-line consecutivos. O cliente paga on-line 3 vezes consecutivamente e/ou o GUI não foi ativado ou seu telefone móvel foi alterado para um tipo que não suporta tal serviço. Depois da desativação, o cliente receberá um SMS dizendo se ele deve ou reativar o serviço GUI ou utilizar os métodos de dois contatos do processo de transação de pagamento.

Além disso, neste exemplo, o pré-processamento representa uma operação sem contato on-line comum realizada no primeiro posicionamento do cartão 1, neste documento, um telefone móvel no leitor de terminal 2. Durante o pré-processamento, o terminal 2 se apresenta como, por exemplo, tipo de terminal = 12 (terminal POS 2 ocupado por um vendedor). O terminal 2 envia uma requisição para uma autorização on-line ao processador de pagamento 5 (servidor autorizado do banco que emitiu o cartão de pagamento 1). O resultado do pré-processamento é, entre outros, um código de resposta e um certificado do processador de pagamento.

O usuário inicia o pedido de pagamento GUI no telefone móvel. A aplicação solicita uma senha. Se a senha é aplicada, então o terminal POS embutido utiliza a senha para obter o código PIN. O código PIN é armazenado em uma aplicação separada no elemento de segurança. O terminal POS embutido verifica o PIN na aplicação PAYPASS/PAYWAVE e se for válido, configura o pedido de pagamento de forma que durante a transação, nenhuma verificação adicional pelo PIN sobre o Dispositivo de Entrada de PIN (PED) no terminal POS 2 seja solicitada. Uma tecnologia de plataforma de PIN sobre senha é definida por esta configuração. Se o usuário iniciar o pedido de pagamento, mas não introduzir uma senha e o terminal 2 solicitar

uma verificação de PIN, é necessário introduzir PIN sobre PED ou posicionar FOB (transportador de dados externos) próximo ao leitor e enviar para verificação ao processador de pagamento 5. Se o telefone não é equipado com pedido de pagamento GUI, e o terminal 2 solicita verificação PIN, a verificação não será feita on-line no processador de pagamento 5.

O terminal 2 envia Lista de Objeto de Dados de Cartão de Gerenciamento de Risco de Cartão (CDOL 1) e gera primeiro comando CA para o cartão 1. O cartão 1 calcula o ARQC. Se o gerenciamento de risco do terminal 2 solicitar PIN e nenhuma senha for inserida no GUI, o terminal 2 solicita o PIN a ser inserido no Dispositivo de Entrada de Pin (PED) e nesta etapa verifica o PIN on-line. O terminal 2 envia o criptograma ARQC calculado como uma solicitação para autorização on-line ao processador de pagamento 5. O processador de pagamento 5 envia de volta a resposta (criptograma ARPC) adicionado por um código de resposta e um certificado.

O pós-processamento executa o segundo posicionamento do cartão próximo ao terminal 2 quando o terminal 2 envia o código de resposta e o certificado ao cartão 1 para o próximo processamento, como a seguir.

1. Depois que o terminal 2 recebe o criptograma ARPC do processador de pagamento (fim do pré-processamento), o terminal solicita o usuário para posicionar o cartão 1, o telefone móvel próximo ao leitor sem contato do terminal novamente.

2. Depois de posicionar o cartão 1, o terminal 2 ativa o PAY-PASS/PAYWAVE_POSTPROCESS e se apresenta não como um tipo de terminal = 12, mas como um tipo de terminal = 27 (Terminal pós-processamento ocupado por um vendedor), respectivamente como um tipo de terminal = 12 tc2.

3. O cartão reconhece este tipo do terminal (que está no processamento de transação de dois contatos), solicita ao terminal 2 dados de CDOL2 para calcular a segunda geração de CA.

4. O CDOL2, a partir do terminal 2, deve abranger, entre outros dados, um código de resposta do processador de pagamento.

5. O terminal 2 envia o certificado ao cartão 1.

6. Durante cálculo, o ARQC, que foi temporariamente armazenado durante o pré-processamento, é utilizado.

7. O cartão envia o TC/AAC calculado ao terminal 2.

Se o usuário não posicionar seu telefone móvel, o dispositivo de comunicação móvel 4, ao leitor pela segunda vez, o terminal reportará ao processador de pagamento 5 que a mensagem de entrega foi malsucedida. O processador de pagamento enviará o ARPC como dados de SMS ao número de telefone em que o cartão SD 1 é inserido (o processador 5 adquire e lembra este número durante ativação de resposta SMS da ativação SMS do GUI). O envio de tecnologia SMS grava o SMS recebido e depois descobre que envolve dados relevantes para o cartão SD, ele executa o terminal POS genérico. Além de outras informações, os dados SMS devem incluir também informações sobre tipo de terminal = 17 (terminal pós-processamento 2 que pertence a uma instituição financeira). O terminal POS genérico lê dados de configuração do terminal padrão no elemento de segurança (o terminal 2 que pertence ao processador de pagamento 5 ou ao processador de pagamento que coopera com o processador 5 do pagamento). Subseqüentemente, o terminal POS embutido inicia o PAY-PASS/PAYWAVE_POSTPROCESS e se apresenta como tipo de terminal = 17. O cartão 1 reconhece o tipo do terminal (que está na plataforma de processamento de transação de dois contatos), solicita o terminal 2 por dados CDOL2 (que contém ARPC) para calcular a segunda geração de CA. O terminal 2 envia um certificado no cartão 1. O ARQC, que foi temporariamente armazenado durante o pré-processamento, é utilizado para calcular mais tarde. O cartão 1 envia o TC/ACA calculado como uma resposta ao terminal 2. O terminal 2 decodifica a resposta e armazena na memória de onde o GUI a pega e envia como uma resposta ao anfitrião do processador 5 do pagamento enquanto reconhece o número de telefone da RESPOSTA SMS recebida.

Quando o cartão 1 recebe o ARPC do processador de pagamento 5, ele ajusta o LATC que o capacita a realizar outros "n" (ilimitados) pagamentos off-line e não importa se é sobre resposta SMS ou sobre segundo

contato. Se o usuário recusa o segundo contato na plataforma de dois contatos e/ou resposta SMS não é ativada, ele não será capaz de realizar pagamentos off-line. Porém, ele pode ainda pagar, mas apenas com autorização on-line, no processador de pagamento 5. As transações off-line serão permitidas depois que o ARPC (resposta) é recebido corretamente do processador de pagamento 5. Assim, ele será permitido pagar novamente um número ilimitado de vezes, naturalmente, sob a condição de que exista dinheiro off-line suficiente no cartão do usuário.

Aplicabilidade industrial

10 A aplicabilidade industrial é óbvia. De acordo com esta invenção, é possível criar e utilizar sistemas para aplicações de pagamento eletrônico em que uma transação de pagamento é dividida em duas fases que capacitam a interrupção de uma ligação de comunicação entre um cartão de um terminal.

15 Lista de símbolos relacionados:

- 1- um cartão
- 2- um terminal de pagamento
- 3- uma ligação de comunicação
- 4- um dispositivo de comunicação móvel
- 20 5- um processador de pagamento
- 6- um trajeto de comunicação
- 7- um elemento de comunicação
- POS – ponto de venda
- ACA – Criptograma de Autenticação de Aplicação
- 25 ARQC – Criptograma de Solicitação de Autorização
- ARPC – Criptograma de Resposta de Autorização
- CDOL - Lista de Objeto de Dados de Gerenciamento de Risco de Cartão
- TC – Certificado de Transação
- POS 12 – ponto de venda ocupado por um vendedor
- 30 POS 12tc2 – ponto de venda ocupado por um vendedor no pós-processamento – com capacidade de terminal diferente
- EMV - Europay, MasterCard, VISA

REIVINDICAÇÕES

1. Método de transação de pagamento eletrônico com a utilização de um meio de pagamento sem contato que inclui um procedimento durante o qual um arquivo de pagamento, especialmente sob a forma de ARQC, é criado pelo cartão (1) e eletronicamente assinado no cartão (1) com o uso de dados de pagamento, principalmente sob a forma de CDOL, que são recebidos do terminal de pagamento (2) depois do reinício do cartão (1), sendo que o arquivo de pagamento é enviado pela ligação de cartão (1) com o terminal de pagamento (2) ao processador (5), e subsequente-mente, o cartão (1) recebe de volta o arquivo de resposta do processador (5), que é principalmente do tipo ARPC e que, sob a forma decodificada, contém dados sobre o arquivo de pagamento, sendo que o cartão (1) processa o arquivo de resposta e, conseqüentemente, define e envia ao terminal (2) uma declaração de aceitação ou rejeição de um pagamento, principalmente sob a forma de TC ou AAC, caracterizado pelo fato de que, durante o processamento de uma transação de pagamento, a ligação de comunicação (3) entre o cartão (1) e o terminal (2) é interrompida e, após a ligação de comunicação (3) entre o cartão (1) e o terminal (2) ser interrompida, um arquivo de resposta do processador de pagamento (5) é recebido no cartão (1); sendo que duas fases do processamento de transação de pagamento são separadas por um reinício do cartão de pagamento, de modo que, na segunda fase, dados criados no cartão (1) antes da interrupção da ligação de comunicação (3) sejam utilizados.

2. Método de transação de pagamento eletrônico, de acordo com a reivindicação 1, caracterizado pelo fato de que o arquivo de pagamento assinado eletronicamente, principalmente sob a forma de ARQC, é armazenado na memória do cartão (1) pelo menos até o arquivo de resposta correspondente ser recebido pelo processador de pagamento (5), principalmente sob a forma de ARPC, sendo que o cartão (1) decodifica o arquivo de resposta recebido e adquire informações sobre o arquivo de pagamento que foi utilizado para criar o arquivo de resposta e, subsequentemente, o cartão (1) cria uma declaração de aceitação ou rejeição do pagamento.

3. Método de transação de pagamento eletrônico, de acordo com a reivindicação 2, caracterizado pelo fato de que o cartão (1) compara um arquivo de pagamento originalmente criado que é armazenado no cartão (1) a um arquivo de pagamento que é incluído no arquivo de resposta.

5 4. Método de transação de pagamento eletrônico, de acordo com qualquer uma das reivindicações 1 a 3, caracterizado pelo fato de que a declaração de aprovação direcionada ao pagamento é criada no cartão (1) sob a condição de que o arquivo de pagamento originalmente criado e armazenado no cartão (1) seja idêntico ao arquivo de pagamento que está no
10 arquivo de resposta.

5. Método de transação de pagamento eletrônico, de acordo com qualquer uma das reivindicações 1 a 4, caracterizado pelo fato de que, depois de receber o arquivo de resposta, o terminal (2) solicita a restauração da ligação de comunicação (3) entre o cartão (1) e o terminal (2), em que,
15 depois de a ligação de comunicação (3) entre o cartão (1) e o terminal (2) ser restaurada, o cartão (1) solicita ao terminal (2) que reenvie os dados de pagamento acrescentados com uma resposta do processador de pagamento (5).

6. Método de transação de pagamento eletrônico, de acordo com qualquer uma das reivindicações 1 a 5, caracterizado pelo fato de que o
20 cartão (1) é incluído em um cartão de memória removível para um dispositivo de comunicação móvel (4), vantajosamente do tipo micro SD ou mini SD ou SD.

7. Método de transação de pagamento eletrônico, de acordo com qualquer uma das reivindicações 1 a 6, caracterizado pelo fato de que
25 um trajeto de comunicação (6) para a transferência do arquivo de resposta é diferente de um trajeto de comunicação (3) utilizado para a transferência de arquivo de pagamento entre o cartão (1) e o terminal (2).

8. Método de transação de pagamento eletrônico, de acordo com qualquer uma das reivindicações 1 a 7, caracterizado pelo fato de que,
30 depois de receber um arquivo de resposta do processador de pagamento (5), o terminal (2) na segunda fase contata o cartão (1) como um terminal (2)

com uma identificação que é diferente de uma identificação do terminal de pagamento (2) na fase de envio do arquivo de pagamento para o processador de pagamento (5).

5 9. Método de transação de pagamento eletrônico, de acordo com a reivindicação 8, caracterizado pelo fato de que o terminal (2) armazena o arquivo de resposta em preparação para restaurar a ligação de comunicação (3) com o cartão (1).

10 10. Método de transação de pagamento eletrônico, de acordo com qualquer uma das reivindicações 1 a 9, caracterizado pelo fato de que a rede de comunicação móvel é utilizada para enviar o arquivo de resposta, sendo que o arquivo de resposta é recebido pelo cartão (1) através de um dispositivo de comunicação móvel (4) que recebe a mensagem em formato SMS.

15 11. Sistema de transação de pagamento eletrônico particularmente com a utilização de meio de pagamento sem contato que inclui um cartão de pagamento (1) em um dispositivo de comunicação móvel (4), um terminal (2), uma conexão entre um terminal (2) e um processador de pagamento (5), caracterizado pelo fato de que o cartão de pagamento (1) inclui uma memória que tem um arquivo de pagamento armazenado no mesmo,
20 em que o arquivo de pagamento é, também, armazenado na memória depois de um reinício do cartão (1) que prossegue após a interrupção de uma ligação de comunicação (3) do cartão (1) e o terminal (2), em que o terminal (2) inclui a memória para armazenamento temporário do arquivo de resposta que está principalmente sob a forma de ARPC, e o terminal (2) é ajustado
25 para a alteração de seus dados de identificação de registro após o arquivo de resposta ser recebido.

12. Sistema de aplicações de pagamento sem contato, de acordo com a reivindicação 11, caracterizado pelo fato de que a memória do cartão (1) para o armazenamento do arquivo de pagamento é um elemento
30 seguro.

13. Sistema de aplicações de pagamento sem contato, de acordo com a reivindicação 11 ou 12, caracterizado pelo fato de que o cartão

de pagamento (1) é incluído em um cartão de memória removível para um dispositivo de comunicação móvel (4), preferencialmente do tipo micro SD ou mini SD, ou SD.

14. Sistema de aplicações de pagamento sem contato, de acordo com qualquer uma das reivindicações 11 a 13, caracterizado pelo fato de que o cartão de pagamento (1) inclui um elemento de comunicação sem contato (7) para a comunicação com o terminal (2).

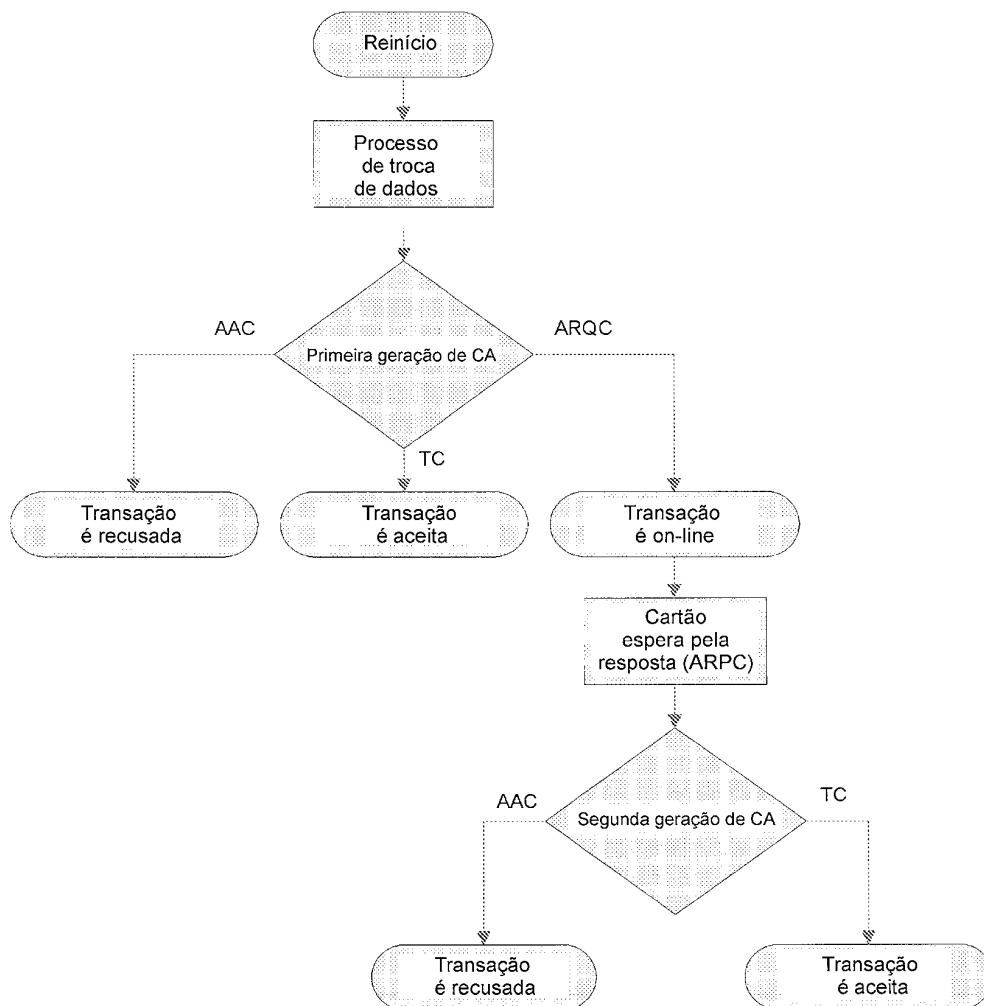


Fig. 1

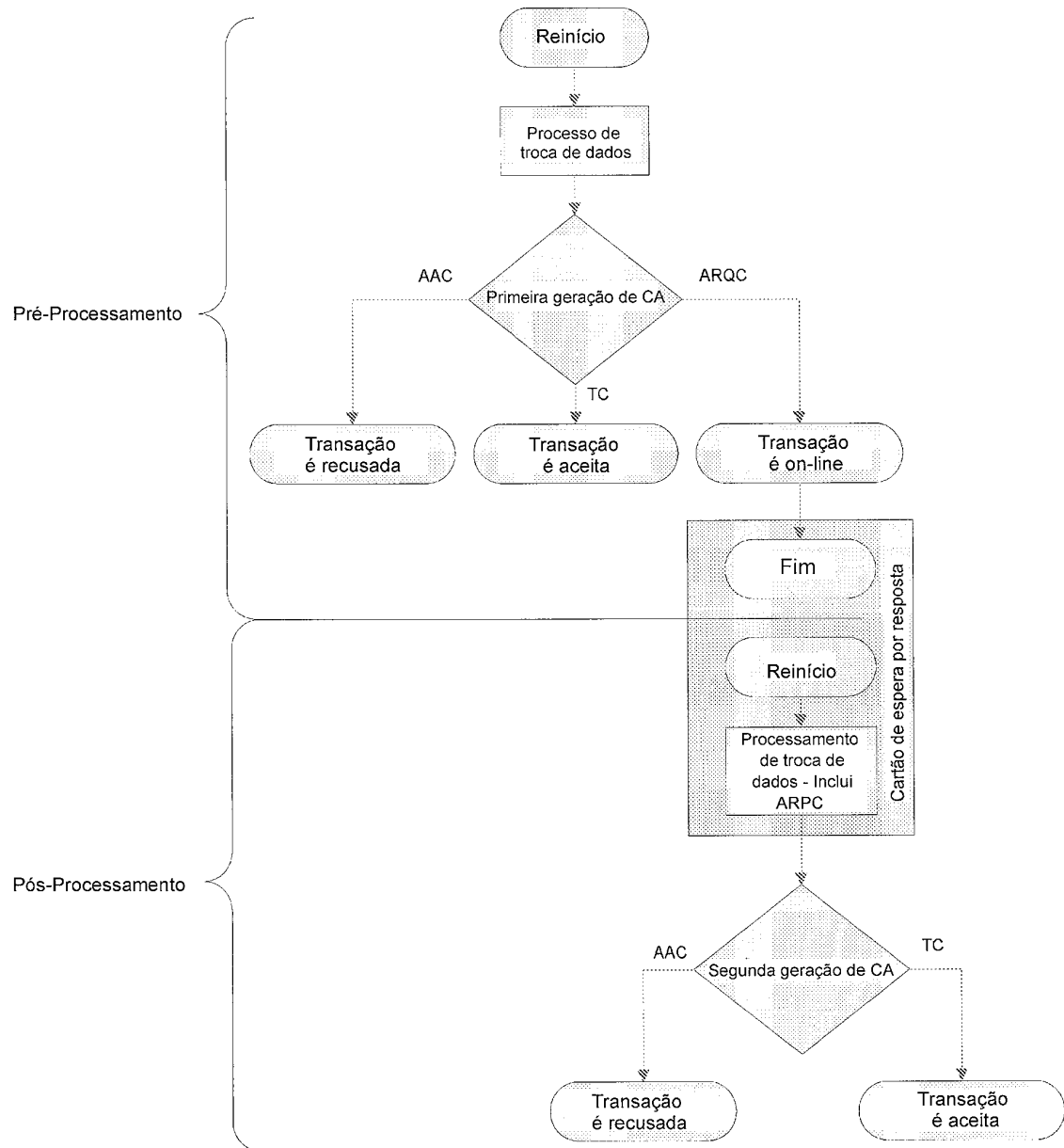


Fig. 2

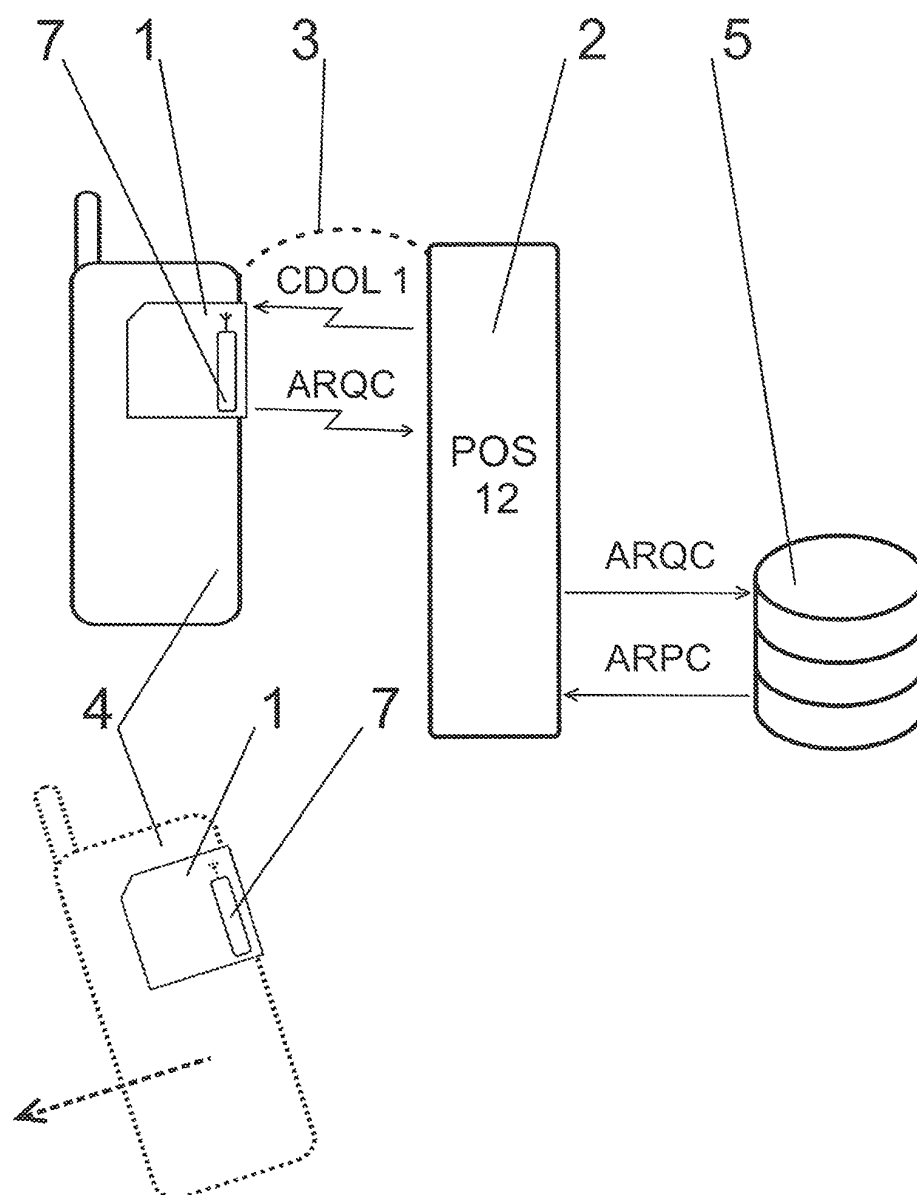


Fig. 3

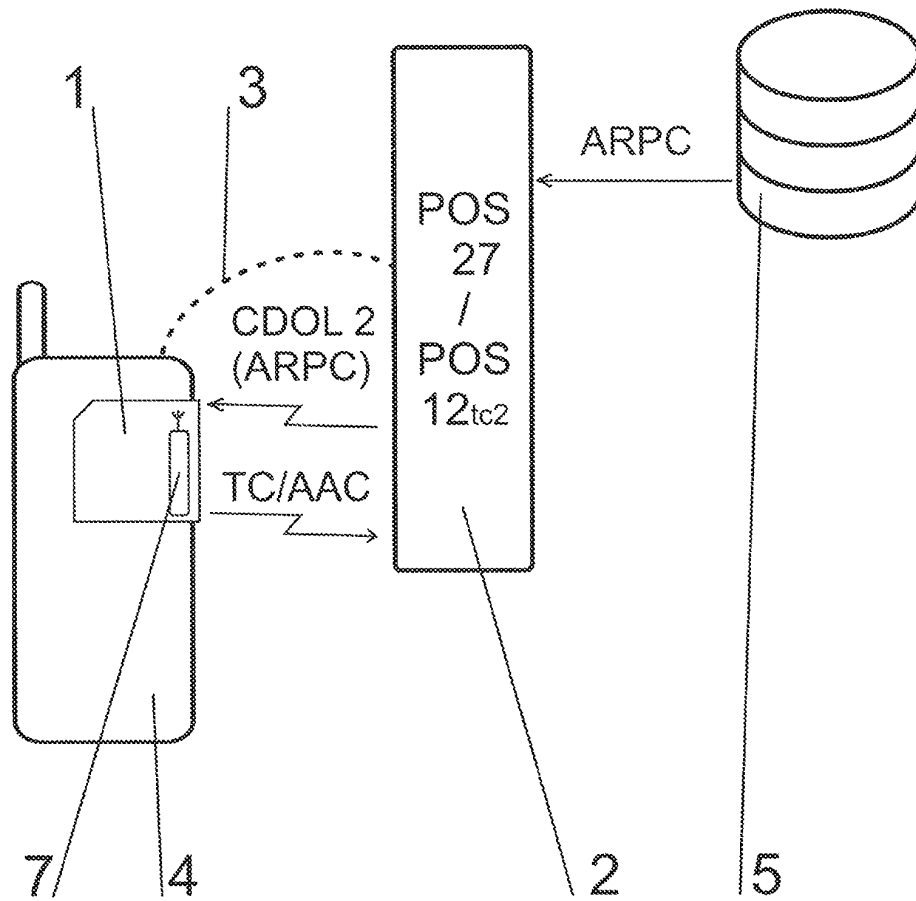


Fig. 4

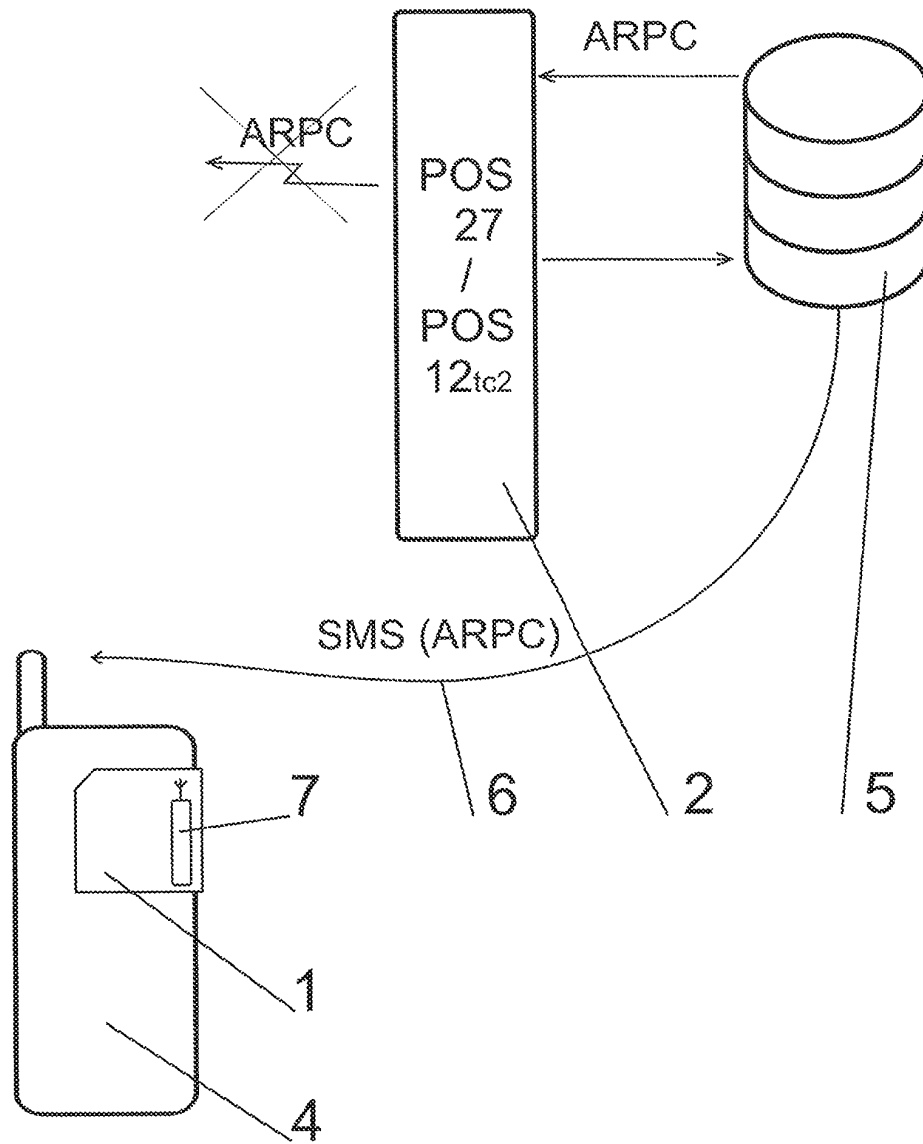


Fig. 5